

AR4



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/692,348	10/19/2000	Bruce Leroy Beukema	AUS9-2000-0631-US1	6902
35525	7590	11/17/2004	EXAMINER	
IBM CORP (YA)			SHIN, KYUNG H	
C/O YEE & ASSOCIATES PC				
P.O. BOX 802333			ART UNIT	
DALLAS, TX 75380			PAPER NUMBER	
			2143	

DATE MAILED: 11/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/692,348

Applicant(s)

BEUKEMA ET AL.

Examiner

Kyung H Shin

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 28 July 2004.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 January 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) *   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>8/16/04, 6/21/04</u> . | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### *Response to Amendment*

1. This action is responding to application papers dated 10/19/2000.
2. Claims **1-25** are pending. Claims **1, 6, 7, 9-13, 18, 19, 21-25** are amended.  
Claims 1, 10, 12, 13, 22, 24, 25 are independent

### *Response to Arguments*

3. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.
4. The text of Title 35, U.S. Code not included in this action can be found in a prior Office action.

## REMARKS

5. In response to applicant's arguments:
  5. 1. The Applicant states that the combination of Williams-Frezza would not have been obvious.

The usage of a security (i.e. encryption) or an access control mechanism in a network environment can utilize a key as the principal requirement for operation. The transfer of the key between two network nodes is a requirement for the utilization of this type of system. There are several mechanisms for the transfer of a key (i.e. partition access key) between two network nodes: (1) a Certificate Authority (i.e. a trusted 3<sup>rd</sup> party) used for key transfer; (2) transfer the key utilizing an in-band (i.e. network

Art Unit: 2143

communications) method; (3) transfer the key utilizing an out-band (i.e. non-network based communications) method; or (4) utilization of a key exchange algorithm. It would have been obvious to select any one of these methods for the key transfer.

Williams-Frezza discloses a network management and access control system that monitors and controls access (i.e. key usage) to a network. Williams discloses the transfer of an access control (i.e. partition key) mechanism. Williams-Frezza discloses an in-band method (i.e. key transfer using network communications) for the key transfer. The combination of Williams and Frezza is obvious due to the requirement to transfer a key between network nodes. The applicant disclose an access control mechanism that transfer an access control key. The two systems disclose access control mechanisms utilizing a key for access and a key transfer method, therefore, the two systems are equivalent. The usage of Williams in view of Frezza under USC 103(a) is a valid and obvious combination.

5.2. The applicant states that Williams does not disclose a monitoring event parameter that counts the number of key mismatches encountered and performs a specific action when a threshold value is surpassed.

Network management techniques such as event monitoring are well known and obvious addition for any network resources management system. Event auditing techniques such as updating a count or logging of event occurrences are standard network management concepts. Williams discloses the auditing and logging of

Art Unit: 2143

monitored events by a network management system. Williams does not specifically disclose the update of a counter monitoring a count of a specific monitored event (i.e. key mismatch) occurrences, however, Williams-Kekic discloses a network management system monitoring events and updating a count of any monitored parameter (i.e. key mismatch) and performing a specific action when a pre-determined threshold is surpassed. The applicant invention discloses the update of a count at the occurrence of a key mismatch and a pre-determined action is performed when a threshold value is surpassed. The two systems disclose monitoring a count of an specific event occurrences and an action performed when a threshold is surpassed, therefore both systems are equivalent. (see Kekic col. 27, lines 12-18: “... *testing whether a network management variable value has exceeded some threshold value. The specified actions can include, for example changing a component's state, executing a server operating system command, forwarding a trap to another host, and/or logging pertinent information ...*”)

5.3. Applicant states that the Williams reference does not disclose a partitioned network environment that utilizes shared network resources.

Network resource sharing techniques (i.e. concurrent access between two or more clients), which reduce operational costs and the total number of required network resources, are well known concepts in a network. A partitioned network enables distributed network nodes to access shared network resources such as disk devices. The implementation of shared resources within a distributed network is an obvious and

Art Unit: 2143

effective requirement. Williams does not specifically disclose a partitioned network, however, Williams-Mackenzie discloses a secure partitioned network utilizing shared devices. The applicant invention discloses a partitioned network that enables access to shared devices. The two systems disclose secure network environments utilizing shared devices, therefore, both systems are equivalent.

(see MacKenzie col. 4, lines 41-45: “... a set of computers (also called servers or nodes) that are connected to communication networks and often shared devices to allow the set of computers to interact in a coherent manner ...”; col. 4, lines 48-52: “... nodes in the cluster are also connected to one or more shared storage resources, typically shared disk devices) ...” ; col. 5, lines 34-44: “... recognize the existence of a partitioned cluster condition ... maintaining cluster state information on a shared storage device, such as a disk; utilizing this data to determine the cluster communication connectivity ... of a network partition ...”)

### ***Claim Rejections - 35 USC § 103***

6. **Claims 1-4, 7-16, 19-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Williams et al.** (US Patent No. 6,304,973: Multi-level security network system) in view of **Frezza et al.** (US Patent No. 4,638,356: Apparatus and method for restricting access to a communication network) and further in view of **MacKenzie et al.** (US Patent No. 6,363,495: Method and apparatus for partition resolution in clustered computer systems).

**Regarding Claims 1, 10, 13, 22, 24, 25,** Williams discloses a node, a method in a node and computer program product for managing authorized attempts to access the node or accessing violations, the method comprising:

- c) dropping the packet without a response to the source if the first key does not match the second key; (see col. 22, lines 48-52: *Due to access violation (first key does not match second key) packet processing is stopped and no indication is returned to the source. )*
- d) storing information from the packet; (see col. 17, lines 19-27: *During audit processing, information from the packet is stored. )*
- e) sending the information to a selected recipient in response to a selected event. (see col. 5, lines 39-41; col. 17, lines 19-27: *All Network accesses are monitored and selected event are audited. During the audit process a selected recipient is sent information concerning the audited event. )*

Williams discloses a secure network environment controlling access to distributed network nodes. (see Williams col. 4, lines 28-33: *"... provide a centralized administration of a layer 3 secure network ... distributed over the Internet ... provide a security device that prevents unauthorized third parties from gaining access to a host ..."*)

Network resource sharing techniques, which reduce operational costs due to a reduction in the total number of required network resources, are

well known concepts for a network. A partitioned network enables network nodes to access shared network resources such as disk devices. The implementation of shared resources within a distributed network is an obvious and efficient addition to any network.

Williams-Frezza does not specifically disclose a partitioned network, however, **Williams-Frezza in view of Mackenzie** discloses a secure partitioned network utilizing shared devices. The applicant's invention discloses a partitioned network that enables access to shared devices. The two systems disclose partitioned networks utilizing shared devices, therefore, both systems are equivalent.

- a) receiving a packet from a source, wherein the packet includes a first key,  
wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node; (see Frezza, col. 6, lines 37-44; MacKenzie, col. 4, lines 48-52: nodes have access to shared disk drives)
- b) determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node; (see Frezza, col. 2, lines 40-51; MacKenzie, col. 5, lines 7-8: network partition techniques)

Williams discloses receiving a packet from a source and verifies an authorized IP address (see col. 22, lines 48-52), but does not explicitly teach an authentication process with a node key in packet. However, Frezza discloses in "Apparatus and Method for restricting access to a Communication Network", an authentication process that involves restricting access to a network with a node key, whereby the key is stored in the header of network packet. (see Frezza, col. 6, lines 37-44)

The key is used to determine whether they are valid to access to a network (e.g. frame verifier, FV, codes), then if the items match authentication is successful. (see Frezza, col. 2, lines 40-51)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Williams** with a packet contains a key to determine whether they are valid as taught in **Frezza**, and to utilize network partitioning techniques as taught by **MacKenzie**. One would have been motivated to include a node key that is transmitted within the network packet as in Frezza in order to have the strengthened authentication process by restricting access to unauthorized attempts on the network, and MacKenzie's for efficient utilization of network resources. (see MacKenzie col. 4, lines 48-52: "*... nodes in the cluster are also connected to one or more shared storage resources, typically shared disk devices. During normal operation, programs running on each node will read and write data to the shared device(s)...*"; col. 5, lines 34-44: "*... recognize the existence of a partitioned cluster condition ... maintaining cluster state information on a shared storage device ...*

Art Unit: 2143

*making a determination of the desired cluster membership in the event of a network partition... ”)*

**Regarding Claims 2, 14,** Williams discloses the method of claim 1 and 13, wherein the selected event is a request from the recipient for the information. (see col. 5, lines 51-55; col. 18, lines 11-19: *Access violations, security related events, are reported to Network Security Controller (NSC) and are transmitted to audit process which is designated as a recipient.*)

**Regarding Claims 3, 15,** Williams discloses the method of claim 1 and 13, wherein the selected event is an occurrence of a trap. (see col. 17, lines 19-27: *The occurrence of a trap, which is designated an interrupt on Page 23 of specification, initiates audit process. Exception events are audited*)

**Regarding Claims 4, 16,** Williams discloses the method of claim 1 and 13, wherein the selected event is a periodic event. (see col. 17, lines 19-27: *Audit process tracks events occurring at a periodic interval such as an exception event.*)

**Regarding Claim 7, 19,** Williams does not specifically disclose a partitioned network, however, **Williams in view of Mackenzie** discloses the method of claim 1 and 13, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network. (see Williams col. 27, lines 38-47: *Alternate embodiment modifies NSC to retrieve access*

Art Unit: 2143

*key for a node from a principal such as a subnet manager. Subnet manager is a SAN device used to configure and manage devices. The partition key is transmitted from the subnet manager to the manager software for inclusion in the authentication process; MacKenzie, col. 4, lines 48-52.)*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Williams** to utilize network partitioning techniques as taught by **MacKenzie**. One would have been motivated to include MacKenzie's for efficient utilization of network resources. (see MacKenzie col. 4, lines 48-52; col. 5, lines 34-44)

**Regarding Claims 8, 11, 20, 23**, Williams discloses the method of claim 1, 10, 13 and 22, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address. (see col. 17, lines 19-27: “ ... detailed information about the individual packets transmitted and received ... “ Key value information in network packets is audited. The subnet manager transmits an identifier (source local, destination local, global identifier address) or a key value to the manager software for inclusion in the authentication process. )

**Regarding Claim 9, 21**, Williams discloses the method of claim 7 and 19, wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet. (see col. 17, lines 19-27; col. 27, lines 38-47: *Alternate embodiment modifies NSC to send*

*audit information concerning access violations to principal such as a subnet manager.*

*The network manager transmits the required information to the subnet manager controlling the SAN.)*

**Regarding Claim 12,** Williams discloses a data processing system comprising:

a) a bus system; a channel adapter unit connected to a system area network fabric; memory includes as set of instructions; (see col. 18, lines 44-50) and

b) a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node; (same as 1.a); determine whether the first key matches a second key for the node (same as 1.b); drop the packet without a response to the source if the first key does not match the second key (same as 1.c); store information from the packet (same as 1.d); and send the information to a selected recipient in response to a selected event. (same as 1.e) These limitations encompass the same scope of the invention as that of the claim 1. a - e, therefore these limitations are rejected for the same reason as the claim 1. a - e.

**7. Claims 5, 6, 17, 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Williams-Frezza-MacKenzie as applied to claims 1, 13 above, and **further in view of Kekic et al. (US 6,664,978).**

Williams discloses a secure network environment controlling access to distributed network nodes. (see Williams col. 4, lines 28-33: “... *provide a centralized administration of a ... secure network ... provide a security device that prevents unauthorized third parties from gaining access to a host ...*”) Network management techniques such as event monitoring, logging and event parameter update are obvious additions for the management of network resources. Williams does not specifically disclose updating a counter value at the occurrence of a monitored events (i.e. key mismatches), however, **Kekic** discloses a network management system monitoring events and updating a counter value for a monitored parameter (i.e. key mismatches) and performing a specific action when a pre-determined threshold is surpassed. The applicant invention discloses the update of a counter of key mismatch events and a pre-determined action being performed when a threshold value is surpassed. The two systems disclose monitoring event occurrences and performing pre-determined actions when a threshold is surpassed, therefore, both systems are equivalent.

**Regarding Claim 5, 17, Kekic** discloses the method of claim 1 and 13 further comprising: incrementing a counter source if the first key does not match the second key. (see Kekic col. 27, lines 12-18; col. 69, lines 58-59: counter value is updated when event (key mismatch) is encountered)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Williams to include the ability to update a count of key mismatches as taught by Kekic. One of ordinary skill in the art would be motivated to

Art Unit: 2143

enhance Williams in order to perform event driven network management activities.

(see Kekic col. 4, line 66 - col. 5, line 4: “ ... *standards-based network management solution for computer networks having a computer network management capability. The managed element server of this invention efficiently manages a constantly changing and growing heterogeneous computer network ...*”)

**Regarding Claim 6, 18,** Kekic discloses the method of claim 5 and 17, wherein the selected event occurs when the counter source exceeds a threshold value. (see col. 27, lines 12-18; col. 69, lines 58-59: counter value triggers a specific action when a threshold value is surpassed)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Williams to include the ability to update a key mismatch counter and perform a specific action when a threshold value is surpassed as taught by Kekic. One of ordinary skill in the art would be motivated to enhance Williams in order to perform event driven network management activities. (see Kekic col. 4, line 66 - col. 5, line 4: “ ... *standards-based network management solution for computer networks having a computer network management capability. The managed element server of this invention efficiently manages a constantly changing and growing heterogeneous computer network ...*”)

#### **Contact Information**

Art Unit: 2143

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS

Kyung H Shin  
Patent Examiner  
Art Unit 2143

KHS  
Nov. 7, 2004

William C. Vaughn  
Primary Examiner  
Art Unit 2143  
William C. Vaughn